INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-11 19:26 UTC

Ubiquiti UniFi OS Server Command Injection via Improper Input Validation (CVE-2026-34910)

CVE VULNERABILITY | CRITICAL | CVSS 9.8 | CISA KEV

SCC Item ID	SCC-CVE-2026-0295
Type	CVE Vulnerability
CVE ID	CVE-2026-34910
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.1815 (95th percentile)
KEV Status	Yes — CISA Known Exploited Vulnerability
Affected Products	Ubiquiti Inc UniFi OS Server (specific version range unconfirmed, verify via Ubiquiti security advisories)
Published	2026-06-09T00:00:00Z
Discovery Source	Vulncheck Kev

Executive Summary

A critical command injection vulnerability in Ubiquiti UniFi OS Server allows an unauthenticated attacker with network access to execute arbitrary operating system commands on affected devices. UniFi OS underpins Ubiquiti's widely deployed network management infrastructure, including routers, switches, and access points used across enterprise, campus, and distributed branch environments. With a CVSS score of 9.8 and confirmed active exploitation in both the CISA and VulnCheck Known Exploited Vulnerabilities catalogs, this vulnerability represents an immediate risk of full device compromise, lateral movement, and loss of visibility and control over network infrastructure operations.

Technical Analysis

CVE-2026-34910 is an Improper Input Validation vulnerability (CWE-20) enabling Command Injection (CWE-77) in the UniFi OS Server component on Ubiquiti UniFi OS devices. An unauthenticated attacker with network-level access to the affected service can inject and execute arbitrary operating system commands. The vulnerability maps to MITRE ATT&CK T1190 (Exploit Public-Facing Application) for initial access and T1059 (Command and Scripting Interpreter) for execution. CVSS base score is 9.8. EPSS score is 0.181 (95th percentile), indicating high probability of exploitation in the wild. The vulnerability appears in both CISA KEV and VulnCheck KEV catalogs, confirming active exploitation. Specific affected version ranges are unconfirmed at pipeline time,

consult Ubiquiti security advisories directly for authoritative version scope. A second related identifier, CVE-2026-34908, is referenced in consolidated source data; its relationship to this vulnerability should be clarified via official Ubiquiti advisories.

Action Checklist

1. Step 1: Containment, Immediately restrict network access to UniFi OS management interfaces (default ports include TCP 8080, 8443, 8880, 8843) using perimeter firewall rules and host-based firewall controls (NIST AC-17; CIS 4.4, CIS 4.5). Remove UniFi OS management interfaces from internet exposure if not already behind a VPN or jump host. Prioritize devices where the management interface is directly reachable from untrusted networks.
2. Step 2: Detection, Review UniFi OS device system logs and network flow data for anomalous command execution patterns, unexpected outbound connections from UniFi controllers, and unusual process spawning from the UniFi OS Server process. Look for shell interpreter invocations (sh, bash, cmd) as child processes of the UniFi service. Correlate against CISA KEV catalog entry for CVE-2026-34910 and check network perimeter logs for scanning activity targeting UniFi management ports. Enable audit logging per NIST AU-2 and AU-12 if not already active (CIS 8.2).
3. Step 3: Eradication, Apply the vendor-issued patch for CVE-2026-34910 as published in the official Ubiquiti security advisory (check https://community.ui.com/releases or consult Ubiquiti's official security page directly for the most current patched version; do not rely on this document for version numbers). If a patch is unavailable for your deployed version, apply compensating controls: disable remote access to the management interface, enforce allowlist-only network access (NIST AC-4; CIS 4.2), and rotate all UniFi OS administrative credentials immediately (MITRE D3FEND D3-CRO).
4. Step 4: Recovery, After patching, validate that the UniFi OS Server service is running the patched version. Audit all UniFi OS administrative accounts for unauthorized additions or privilege changes (NIST AC-2; MITRE D3FEND D3-LAM). Review system file integrity for evidence of persistence mechanisms such as modified startup configurations (MITRE D3FEND D3-SICA, D3-SFA). Restore management interface access only after confirming patch installation and reviewing logs for signs of prior compromise. Re-enable monitoring with enhanced logging retention (NIST AU-11).
5. Step 5: Post-Incident, Document the gap that allowed UniFi OS management interfaces to be network-accessible without authentication controls. Update network segmentation policy to enforce management-plane isolation for all network infrastructure (NIST AC-4, AC-6; CIS 4.2). Ensure UniFi OS devices are included in the vulnerability management process with automated patch tracking (CIS 7.1, 7.2, 7.3). Validate that asset inventory reflects all deployed UniFi OS devices (CIS 1.1). Require MFA for all UniFi OS administrative access (NIST AC-17; CIS 6.5; MITRE D3FEND D3-MFA).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership, legal counsel, and executive notification immediately if forensic analysis confirms exploitation occurred prior to containment (indicated by shell child processes, unauthorized accounts, or SSH key injection in UniFi OS), as the CISA KEV listing combined with CVSS 9.8 and unauthenticated remote code execution on network infrastructure management systems meets the threshold for potential breach notification under CIRCIA, state data breach statutes, and sector-specific regulations (HIPAA, PCI DSS) if the UniFi OS controllers manage networks carrying regulated data.
Recovery Notes	After confirming patch installation and clean account/file integrity audit, restore management interface access in phases: first to an isolated administrative VLAN only, then monitor `/usr/lib/unifi/logs/server.log` and process trees continuously for a minimum of 72 hours before re-enabling any broader access. Given that CVE-2026-34910 is actively exploited and UniFi OS manages the underlying network fabric, treat any anomalous outbound connection from the controller host (particularly to non-Ubiquiti cloud IPs) during the recovery window as a recompromise indicator requiring immediate re-isolation. Retain enhanced log verbosity and a 90-day minimum retention window for all UniFi OS logs for the 6 months following recovery.
Forensic Artifacts	UniFi OS Server application log at /usr/lib/unifi/logs/server.log — review for HTTP requests to the management API containing shell metacharacters (|, ;, $(), backticks) in URI parameters or POST body fields, which represent the direct injection payload for CVE-2026-34910 | Linux process tree snapshot (ps auxf output) and auditd execve syscall logs filtered on the UniFi service UID — shell interpreter processes (sh, bash) spawned as children of the UniFi service binary are the primary runtime indicator of successful command injection exploitation | Crontab entries for all system users (crontab -l, /etc/cron.d/, /etc/cron.hourly/) and /etc/rc.local, ~/.bashrc, and ~/.profile for all users — command injection exploitation of network device management platforms commonly establishes cron- or init-based persistence immediately after initial access | SSH authorized_keys files for all OS-level user accounts (find /home /root -name authorized_keys) and /etc/passwd for unauthorized local account additions — unauthenticated RCE against UniFi OS at CVSS 9.8 with active exploitation strongly suggests automated post-exploitation frameworks that deposit SSH keys as a persistence mechanism | Network flow records (NetFlow, sFlow, or firewall connection logs) for the UniFi controller host filtered to outbound connections on non-standard ports during the exposure window — command injection payloads frequently initiate reverse shells or download stagers, producing outbound connections to attacker-controlled infrastructure that will appear in perimeter flow data even after the host is patched

Per-Action IR Details

Step 1: Containment — Immediately restrict network access to UniFi OS management interfaces (default ports include TCP 8080, 8443, 8880, 8843) using perimeter firewall rules and host-based firewall controls (NIST AC-17; CIS 4.4, CIS 4.5). Remove UniFi OS management interfaces from internet exposure if not already behind a VPN or jump host. Prioritize devices where the management interface is directly reachable from untrusted networks.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On Linux-based UniFi OS hosts, immediately apply iptables rules to restrict access to TCP 8080, 8443, 8880, and 8843: `iptables -I INPUT -p tcp --dport 8080 -s -j ACCEPT && iptables -I INPUT -p tcp --dport 8080 -j DROP` (repeat for each port). On the perimeter, use pfSense or iptables on a border device to block these ports from all untrusted source ranges. Document each rule with timestamp and approver for audit trail.

Evidence: Before applying firewall rules, capture all active TCP connection state from the UniFi OS host: run `ss -tnp` or `netstat -ano` to record established sessions on ports 8080, 8443, 8880, and 8843, noting remote IP addresses that may indicate active exploitation or C2 channel. Also capture `ps auxf` output to identify any shell processes (sh, bash) currently running as children of the UniFi service process — these would be direct indicators of in-progress command injection exploitation. Save outputs with timestamps before any rule changes alter or terminate live sessions.

Step 2: Detection — Review UniFi OS device system logs and network flow data for anomalous command execution patterns, unexpected outbound connections from UniFi controllers, and unusual process spawning from the UniFi OS Server process. Look for shell interpreter invocations (sh, bash, cmd) as child processes of the UniFi service. Correlate against CISA KEV catalog entry for CVE-2026-34910 and check network perimeter logs for scanning activity targeting UniFi management ports. Enable audit logging per NIST AU-2 and AU-12 if not already active (CIS 8.2).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon on any Windows-based UniFi controller hosts using the SwiftOnSecurity baseline config, filtering for Event ID 1 (Process Create) where ParentImage matches the UniFi service binary and Image contains `sh.exe`, `bash.exe`, or `cmd.exe`. On Linux-based UniFi OS devices, use `auditd` with a rule targeting execve syscalls from the UniFi service UID: `-a always,exit -F arch=b64 -S execve -F uid= -k unifi_exec`. Collect UniFi OS application logs from `/var/log/` and UniFi controller logs from `/usr/lib/unifi/logs/server.log`, grepping for HTTP request patterns containing shell metacharacters (`|`, `;`, `$(`, `` ` ``) in request URIs or POST body fields processed by the management API.

Evidence: Before enabling or modifying any logging configuration, preserve existing log state: archive `/var/log/syslog`, `/var/log/auth.log`, `/usr/lib/unifi/logs/server.log`, and any rotated logs (`.gz` archives) to an integrity-preserving read-only location using `sha256sum` for chain-of-custody hashing. Capture a memory image using LiME or `dd` of `/proc/kcore` if the host shows active shell children — volatile command injection artifacts (injected command strings, environment variables, file descriptors) will not survive process termination. Also capture current crontab entries (`crontab -l` for all users, `/etc/cron*` directories) and `/etc/rc.local` before any changes, as CVE-2026-34910 exploitation for persistence commonly targets these locations.

Step 3: Eradication — Apply the vendor-issued patch for CVE-2026-34910 as published in the official Ubiquiti security advisory (verify current patched version at https://community.ui.com/releases — do not rely on this document for version numbers; consult the advisory directly). If a patch is unavailable for your deployed version, apply compensating controls: disable remote access to the management interface, enforce allowlist-only network access (NIST AC-4; CIS 4.2), and rotate all UniFi OS administrative credentials immediately (MITRE D3FEND D3-CRO).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-4 (Information Flow Enforcement), NIST SI-2 (Flaw Remediation), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If patching is blocked by a change freeze or unavailable for the deployed version, implement the following layered compensating controls achievable without enterprise tooling: (1) Add an nginx or HAProxy reverse proxy in front of the UniFi management ports with strict input validation rejecting requests containing shell metacharacters in URI and body fields; (2) Enforce IP allowlist at the host firewall to permit only dedicated management workstation IPs to reach TCP 8080/8443/8880/8843; (3) Rotate all UniFi OS admin credentials via the UI or CLI (`ubnt-tools` where available) and invalidate all active sessions. Document these compensating controls with a target remediation date per CIS 7.2.

Evidence: Before applying the patch or rotating credentials, capture a full volatile state snapshot: acquire RAM image using LiME if active compromise indicators are present, run `ps auxf` to record all running processes, capture `ss -tnp` for active connections, dump current UniFi OS admin account list via the management API or database query (`mongo ace --quiet --eval 'db.admin.find({},{name:1,email:1,last_site_name:1})'` on self-hosted controllers) to establish a pre-patch baseline for later comparison, and preserve all log files under `/usr/lib/unifi/logs/` with SHA-256 hashes. Credential rotation alters authentication state — any sessions active at rotation time that persist afterward are strong indicators of session token theft or secondary persistence.

Step 4: Recovery — After patching, validate that the UniFi OS Server service is running the patched version. Audit all UniFi OS administrative accounts for unauthorized additions or privilege changes (NIST AC-2; MITRE D3FEND D3-LAM). Review system file integrity for evidence of persistence mechanisms such as modified startup configurations (MITRE D3FEND D3-SICA, D3-SFA). Restore management interface access only after confirming patch installation and reviewing logs for signs of prior compromise. Re-enable monitoring with enhanced logging retention (NIST AU-11).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Validate patch installation by checking the UniFi OS version via `ubnt-tools version` or from the device UI under Settings > System > Updates, cross-referencing against the patched version confirmed in the Ubiquiti security advisory. For account integrity verification without a SIEM, export the admin account list from the UniFi controller MongoDB instance (`mongo ace --eval 'db.admin.find()'`) and diff it against your pre-incident baseline captured during eradication. For file integrity checking without enterprise tooling, run `sha256sum` against known-good hashes of UniFi OS binaries under `/usr/lib/unifi/` and check `/etc/cron*`, `/etc/rc.local`, `~/.bashrc`, and `~/.profile` for all system users for unauthorized additions. Use `find / -newer /var/log/unifi_patch_applied.marker -type f 2>/dev/null` (where the marker file is created at patch time) to surface files modified post-exploitation.

Evidence: Before restoring management interface access, compare current UniFi OS admin account state against the pre-incident baseline: any accounts not present before the exploitation window represent unauthorized additions and must be investigated before recovery proceeds. Audit `/etc/passwd`, `/etc/shadow`, and `/etc/sudoers` for unauthorized local OS accounts created via command injection. Verify SSH authorized_keys files for all users (`find /home /root -name authorized_keys`) — command injection exploitation of UniFi OS commonly deposits SSH keys for persistent access. These artifacts must be reviewed before re-enabling inbound management access, as restoring connectivity to a still-compromised host extends attacker dwell time.

Step 5: Post-Incident — Document the gap that allowed UniFi OS management interfaces to be network-accessible without authentication controls. Update network segmentation policy to enforce management-plane isolation for all network infrastructure (NIST AC-4, AC-6; CIS 4.2). Ensure UniFi OS devices are included in the vulnerability management process with automated patch tracking (CIS 7.1, 7.2, 7.3). Validate that asset inventory reflects all deployed UniFi OS devices (CIS 1.1). Require MFA for all UniFi OS administrative access (NIST AC-17; CIS 6.5; MITRE D3FEND D3-MFA).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management)

Compensating: For asset inventory without enterprise tooling, run an authenticated nmap scan across all RFC 1918 ranges scanning TCP 8080, 8443, 8880, and 8843 (`nmap -sV -p 8080,8443,8880,8843 --open 192.168.0.0/16`) to enumerate all UniFi OS management interfaces on the network — any responding host not in your CMDB represents an inventory gap. Subscribe to the Ubiquiti security advisory RSS feed and CISA KEV catalog updates to automate

patch notification. For MFA enforcement, configure UniFi OS SSO via the Ubiquiti account portal which supports TOTP-based MFA at no additional cost; document this as a required configuration baseline for all future UniFi OS deployments.

Evidence: The primary post-incident forensic deliverable is a documented timeline reconstructed from `/usr/lib/unifi/logs/server.log`, web server access logs, and network flow data showing first contact with the management interface, first exploitation attempt (identified by shell metacharacter payloads in HTTP requests), and the interval between exploitation and containment — this dwell time calculation is required for breach notification threshold analysis and should be preserved for potential regulatory disclosure decisions. Preserve all forensic artifacts collected during detection and eradication phases under legal hold with SHA-256 hash verification, as CISA KEV listing and CVSS 9.8 severity may trigger mandatory reporting obligations depending on sector and jurisdiction.

Detection Guidance

Focus detection on the UniFi OS Server process and management interface traffic. Key indicators: (1) Unexpected child processes spawned by the UniFi OS Server process, particularly shell interpreters (sh, bash) or system utilities (curl, wget, nc), review /proc on Linux-based UniFi hardware or equivalent OS process trees. (2) Outbound connections from UniFi controller hosts to external IPs on non-standard ports, which may indicate reverse shell or C2 beacon activity. (3) Modification of system init or startup files on UniFi OS devices (MITRE D3FEND D3-SICA). (4) Authentication log entries showing new or unknown administrative account creation (MITRE D3FEND D3-LAM). (5) Network perimeter logs showing scanning or probing of UniFi management ports (TCP 8080, 8443) from external sources. Cross-reference any findings against the CISA KEV catalog entry for CVE-2026-34910. Per NIST AU-6, review and analyze system audit records for these indicators at increased frequency until patching is confirmed. No specific IOC hashes or IP indicators were available in the source data for this CVE at pipeline time.

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures

ISO-27001-2022

- **A.8.26** — Application security requirements
- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
vulncheck_kev	https://nvd.nist.gov/vuln/detail/CVE-2026-34910	T1
(consolidated)	https://nvd.nist.gov/vuln/detail/CVE-2026-34908	T1
CVE-2026-34910 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-34910	T3
CVE-2026-34910: UniFi OS Command Injection Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2026-34910/	T3
CVE-2026-3910: Chrome V8 Zero-Day Used for In-the-Wild Attacks	https://socprime.com/blog/cve-2026-3910-vulnerability/	T3
CISA KEV	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

Generated 2026-06-11 19:26 UTC by TJS Security Command Center